State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

March 10, 2015

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2015-022

DATE(S) ISSUED:

03/10/2015

SUBJECT:

Cumulative Security Update for Internet Explorer (MS15-018)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Successful exploitation of these vulnerabilities could result in an attacker gaining elevated privileges on the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE

This advisory covers ten privately disclosed and two publicly disclosed vulnerabilities. Remote code execution vulnerabilities have been identified in eight components of Internet Explorer across multiple Windows products. Microsoft has stated they are aware of the exploit disclosed only one of the two Elevation of Privilege vulnerabilities is being exploited in the wild.

SYSTEM AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8

- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Multiple vulnerabilities were discovered in Internet Explorer due to the way objects in memory are improperly accessed. The vulnerabilities are as follows:

- Nine Memory Corruption Vulnerabilities

- Two Elevation of Privilege Vulnerabilities
- One VBScript Memory Corruption Vulnerability

These vulnerabilities could allow an attacker to execute remote code by luring a victim to a malicious website. When the website is visited, the attacker's script will run with same permissions as the affected user account. Successful exploitation of these vulnerabilities could result in an attacker gaining elevated privileges on the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Microsoft:

https://technet.microsoft.com/en-us/library/security/ms15-018

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0032

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0056

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0072

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0099

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0100

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1622

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1623

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1624

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1625

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1626

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1627

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1634